Office of Administration
Office of Information Technology

Risk Assessment and Management
For
E-Government Program

Version 1.0
December 2000

Table of Contents

1.0 Program Definition

1.1 Definition and Objectives:

The Office of Information Technology is coordinating information technology projects enabling departmental applications of doing business through the Internet. These individual projects will become part of the overall E-Government program. Several departmental applications are being targeted for E-Government (e-government) capabilities including the Department of Revenue Personal Income Tax Filing Systems, Motor Vehicle and Driver's Licensing Systems, Department of Economic Development Workforce System and many others. There may be more than one appropriation created for this project. Each needs to be provided with the PS/EE flexibility. The projects to enable e-government capabilities will require significant manpower exceeding current staffing. Similar to the Y2K project, it is expected that most departments will require contracted IT resources that average around $125-$150 per hour. It has been requested that these appropriations be structured so that departments can hire temporary IT staff (recent retirees perhaps) or to pay for overtime of regular staff. Similar to the Y2K project, this would reduce the hourly rates to the $40-$60 range. Considerable money could be saved if e-government appropriations are flexible to hire temporary IT staff in lieu of contracted staff, as opportunities arise.

1.2 Sponsor and Team:

The Chief Information Officer of the Missouri Office of Information Technology, Gerry Wethington, is the sponsor of this program. Technology Specialist, Jan Grecian is designated as lead program manager and is responsible for execution of the program. Technology Specialist, Bob Meinhardt is the program manager assigned to development of the technical architecture for the program. Technology Specialist, Tom Stokes is the program manager assigned to risk management and oversight of the program.

The Architecture Committee and those identified to develop architecture standards for the proposed project are:

- Mike Schweiss (Department of Health)
- Bob Meinhardt (Office of Information Technology)
- Bob Ordway (Office of State Courts Administrator)
- Chris Wilkerson (Department of Natural Resources)
- Don Lloyd (Department of Economic Development)
- Dustin Bieghler (Secretary of State's Office)
- Gary Lyndaker (Department of Mental Health)
- Jim Branson (Department of Health)
- Mike Miller (Department of Transportation)

- Jim Weber (Department of Revenue)
- John Mullen (Public Defenders Office)
- Lyndon Mote (Department of Agriculture)
- Steve Adams (Department of Social Services)
- Steve White (Department of Elementary & Secondary Education)

The Risk Management Committee and those identified to develop and maintain the risk management plan for the proposed project are:

- Tom Stokes (Technology Specialist - Office of Information Technology)
- Bill Perkins (CIO – Department of Revenue)
- Gina Hodge (Director of Information Technology – Department of Higher Education)
- Don Lloyd (Director of MIS – Department of Economic Development)
- Jan Grecian (Technology Specialist - Office of Information Technology)
- Ritchie Jenkins (IT Project Manager – Department of Revenue)
- Lyndon Mote (Information Technology Supervisor – Department of Agriculture)
- Paul Wright (Acting IT Director – Department of Elementary & Secondary Education)
- Dennis Bax (Acting IT Director – Department of Social Services)
- Larry Lueckenhoff (Programming Analysis Manager – Missouri State Highway Patrol)
- Jearl Reagan (CIO – Department of Labor & Industrial Relations)
- Ron Thomas (Assistant Director, Systems & Programming - Office of Administration)

1.3 Stakeholders:

The implementation team identified the following project stakeholders:

Missouri Citizens
Governor
Legislature
State Employees
State Government Agencies
Federal Government
Courts/Attorney General
Local/County Government
Other States

Foreign Countries
Schools
Banking Industry
Vendors (i.e. IBM, Cisco etc.)
Businesses

1.4 Background:

There is an important need for simplified citizen and business Interaction with Missouri State Government. Several of these business functions require a citizen or private business to interact with several government agencies, often providing the same information to each. E-government should provide a single window into state government eliminating the public or business need to be aware of individual agencies. Missouri citizens and businesses are experiencing an ever-increasing need to transact business with state government 24 hours per day, seven days per week (24/7). Missouri must remain competitive with rapidly expanding government service offerings or risk becoming less attractive from an economic development perspective to corporate entities investigating the possibility of relocating and/or doing business with Missouri.

The e-government initiative is comprised of three categories critical to the ability of Missouri State Government to interact electronically with citizens, businesses and other governmental entities. Those categories consist of (1) an infrastructure capable of supporting the effort and a portal to provide simple access as a "single-point-of-contact", (2) business-to-business (B2B), or government-to-business (G2B) system to allow Missouri State Government to interact with vendors via the Internet, and (3) numerous agency web candidate applications that will provide services to citizens and businesses.

1.5 Goals and Measures:

The Office of Information Technology has established a series of goals to be accomplished over the next two years. Specific goals related to the budget decision item of E-Government projects are:

- Develop a common information technology architecture and standards
- Leverage the state's financial resources through more efficient and effective delivery of services
- Increase customer satisfaction
- Ensure security/privacy
- Simplify products and processes
- Provide information and services on a 24/7 basis
- Upgrade our technology resources

1.6 Phases and Cost Estimates:

The duration of this program is projected over a four-year period with each fiscal year representing a phase. The Office of Information Technology will perform oversight of the program that consists of many projects to be managed by individual state departments and agencies. This program is scheduled to start in FY-2002 with the last phase starting in FY-2005. Following is a list of projects expected to be completed during the first two years along with cost estimates. Detailed descriptions of separate projects may be found in the State of Missouri E-Government Report and Plan published on October 18, 2000.

Cost for the project were estimates taken from the E-Government report and plan completed earlier this year.

FY02 Appropriation Request

Agency	Application	General Revenue	Federal Funds	Professional License Fees	Highway Funds	Lottery Funds	Total
OA	E-Government Infrastructure	6,441,822	0				6,441,822
OA	B2B System	1,988,000	0				1,988,000
DOR	Vehicle Registration Renewal	750,000	0				750,000
DESE	Grants Program	2,250,000	2,250,000				4,500,000
STO	Unclaimed Property	60,000	0				60,000
MDA	Licensing/Loans/Product Marketing, Voting Systems	635,000	0				635,000
DESE	Community Connection	350,000	0				350,000
CBHE	State Grant and Scholarship Applications	0	1,434,000				1,434,000
DED	PR Licensing System	0	0	500,000			500,000
MSHP	Statewide Traffic Accident Records	53,550	0		711,450		765,000
DOLIR	Continued Claims	0	0				0
OIT	GIS System	1,132,182	0				1,132,182
MoDOT	Commercial Vehicle Operations	0	0		600,000		600,000
DPS-DO	Grants Management	0	35,000				35,000
DSS	Employee Disqualification List	225,000	75,000				300,000
Lottery	Web Marketing FY02	0	0			252,504	252,504
DOI	MO Insurance Department System	0	0				0
SOS	Corporation System	0	0				0
DOH	Birth System	200,000	0				200,000
DNR	MO Emissions Inventory System	300,000	0				300,000
Lottery	Retailer Accounts Profile	0	0			162,264	162,264
DSS	Child Support Enforcement	51,000	99,000				150,000
OA	Surplus Property Auction	0	400,000				400,000
DOI	Premium Tax	0	0				0
DPS-FS	Elevator Registration/Inspection	25,000	0				25,000
STO	Linked Deposits	60,000	0				60,000
SOS	Archives & Local Records Holdings	0	0				0
SOS	Centralized Voter Registration DB	0	0				0
DNR	Hazardous Waste Billing System	40,000	0				40,000
Subtotal		**14,561,554**	**4,293,000**	**500,000**	**1,311,450**	**414,768**	**21,080,772**

Continuation of FY02 Appropriation Request Detail

DOI	Surplus Lines	0					0
STO	Check Inquiry	30,000					30,000
Lottery	Retail Licensing	0				25,000	25,000
DPS-FS	Fire Department Registration	15,000					15,000
Lottery	Ticket Validation	0				190,716	190,716
STO	Vendor Electronic Payment Inquiry	30,000					30,000
DOI	Page 14/15 Supplement (4a priority)	0					0
DNR	Public Drinking Water – Surface	20,000					20,000
DOI	Page 15 (backside – 4b priority)	0					0
DPS-SEMA	Training Registration	5,000					5,000
Lottery	Accounts Receivable	0				25,000	25,000
DPS-LC	Licensing	75,000					75,000
DNR	Public Drinking Water – Laboratory	20,000					20,000
MOSERS	Payroll Reporting	0					0
DOI	WC900/IVR System	0					0
DNR	Public Drinking Water – CARES	100,000					100,000
DNR	Publication Sales	40,000					40,000
DOI	Medical Malpractice	0					0
MOSERS	Retirement Benefit Processing	0					0
DPS-LC	Geographicals	50,000					50,000
DNR	Cultural Resource Inventory System	40,000					40,000
DOI	Life Supplement	0					0
DOI	Commercial Liability	0					0
DOI	Products Liability	0					0
DPS-LC	Price Posting	100,000					100,000
Subtotal Page 1		**14,561,554**	**4,293,000**	**500,000**	**1,311,450**	**414,768**	**21,080,772**
Total FY02		**$15,086,554**	**$4,293,000**	**$500,000**	**$1,311,450**	**$655,484**	**$21,846,488**

Y03 Appropriation Request

Agency	Application	General Revenue	Federal Funds	Workers Comp Funds	Highway Funds	Lottery Funds	Total
OA	E-Government Infrastructure	4,722,563					4,722,563
OA	B2B System	448,000					448,000
DESE	Grants	2,250,000	2,250,000				4,500,000
DESE	Community Connection	350,000					350,000
DOLIR	Employer Reporting	0					0
MSHP	MO Uniform Law Enforcement Sys	435,860			711,140		1,147,000
MSHP	Criminal History Record System	725,248					725,248
DOR	Withholding Tax Filing	500,000					500,000
DOLIR	Automated Integrated Claims Sys.	0		475,000			475,000
DOR	Motor Vehicle e-Liens	300,000					300,000
MSHP	Traffic Arrest System/Alcohol Drug Offender Record System	0			1,078,688		1,078,688
DOLIR	Wage Order	150,000					150,000
Lottery	Web Marketing FY03	0				220,000	220,000
Lottery	Telemarketing and Ticket Distribution Retailer	0				50,000	50,000
Lottery	Management Information System	0				125,000	125,000
DOR	Corporate/Franchise Tax Filing	200,000					200,000
DOR	Business Tax Tracking	500,000					500,000
DNR	Rideshare Program	18,000					18,000
DSS/DMH/ DOH/MSHP	Employee Disqualification List/Agency Integration	150,000					150,000
Lottery	Recurring Personnel Costs					**230,484	**230,484
Total FY03		**$10,749,671**	**$2,250,000**	**$475,000**	**$1,789,828**	**$625,484**	****$15,889,983**

**Total varies from E-Government Report and Plan by amount of recurring costs for Lottery personnel.

2.0 Risk Management Methodology:

The following description represents the initial risk plan accomplished for this project. Representatives from agencies with a project budget exceeding $250,000 were used to accomplish this risk assessment. A brainstorming session was held and one hundred thirteen risks were identified for this project. Values were then assigned to the probability (P) of occurrence and to the consequence (C) of occurrence using a scale of 0.0 to 0.9 for each value where zero is the low and 0.9 is high. A risk exposure was calculated by multiplying the probably of occurrence times the consequence of occurrence (PxC). Analysis of the risks led to categorizations based on subjective judgments. Risks were broken into the following twelve categories: Business Process, Communication, Execution, Funding, Legal, Marketing, Resources, Security, Technical, Technology, Training and Vendor. This work is documented in figures 2.1 below:

Initial Risk Identification and Values

Figure 2.1

Ref #	Category	Risk Description	Probability	Consequence	P * C	Risk Levels
1	Business Process	Inadequate organization structure	0.9	0.9	0.81	High
2	Business Process	Lack of ability to identify individual customer and level of access	0.8	0.9	0.72	High
3	Business Process	Lack of business continuity planning	0.6	0.8	0.48	Medium
4	Business Process	Fail to meet customer needs	0.5	0.9	0.45	Medium
5	Business Process	Inability to determine all e-government risks	0.9	0.4	0.36	Medium
6	Business Process	High volatility of business requirements	0.9	0.4	0.36	Medium
7	Business Process	Lack of control due to decentralization	0.8	0.4	0.32	Medium
8	Business Process	Agencies fail to adopt e-government and continue old business practices	0.5	0.6	0.3	Low
9	Business Process	Failure to provide timely information to customers	0.4	0.7	0.28	Low
10	Business Process	State leadership fails to buy in	0.3	0.9	0.27	Low
11	Business Process	Purchasing policies are inadequate to handle e-government	0.2	0.5	0.1	Low

Ref #	Category	Risk Description	Probability	Consequence	P * C	Risk Levels
12	Communication	Conflicts of ownership between agencies	0.9	0.9	0.81	High
13	Communication	Lack of common language between customers, developers and implementers	0.8	0.9	0.72	High
14	Communication	Lack of cooperation between agencies	0.8	0.8	0.64	High
15	Communication	Unwillingness to change - external	0.8	0.6	0.48	Medium
16	Communication	Failure to manage internal government expectations	0.8	0.6	0.48	Medium
17	Communication	Lack of detailed guidance to vendors	0.6	0.6	0.36	Medium
18	Communication	Failure to recognize the value of IT systems	0.5	0.7	0.35	Medium
19	Communication	Poor public perception of e-government initiative	0.4	0.8	0.32	Medium
20	Communication	Communication failure between agencies	0.6	0.5	0.3	Low
21	Communication	Changing demands from legislation	0.2	0.7	0.14	Low
22	Communication	Failure to consider competition from outside sources	0.3	0.3	0.09	Low
23	Communication	Lack of buy in from IT staffs	0.2	0.3	0.06	Low
24	Execution	Lack of sufficient architectural standards	0.9	0.9	0.81	High
25	Execution	No plan for integration of services	0.8	0.8	0.64	High
26	Execution	Failure to establish a unique identifier for each citizen or agency	0.7	0.9	0.63	High
27	Execution	Moving too many applications too fast	0.8	0.7	0.56	Medium
28	Execution	Difficulty of editorial control	0.7	0.7	0.49	Medium
29	Execution	Failure to adequately predict and prepare for growth	0.7	0.7	0.49	Medium
30	Execution	No comprehensive implementation plan	0.6	0.7	0.42	Medium
31	Execution	Failure to manage scope	0.7	0.6	0.42	Medium
32	Execution	Failure to deliver during budget period	0.8	0.4	0.32	Medium
33	Execution	Lack of ability to predict schedule	0.4	0.7	0.28	Low

Ref #	Category	Risk Description	Probability	Consequence	P * C	Risk Levels
34	Execution	Failure to design legislation with Internet in mind	0.4	0.7	0.28	Low
35	Execution	Not enough variety in payment options	0.4	0.7	0.28	Low
36	Execution	No defined metrics for measuring success	0.4	0.7	0.28	Low
37	Execution	No help desk implementation plan	0.3	0.9	0.27	Low
38	Execution	No project manager	0.3	0.9	0.27	Low
39	Execution	Failure to identify completion criteria for agency projects	0.5	0.5	0.25	Low
40	Execution	Failure to deliver services or goods	0.2	0.9	0.18	Low
41	Execution	Failure to comply with ADA requirements	0.3	0.5	0.15	Low
42	Execution	Inability to measure customer goodwill	0.5	0.3	0.15	Low
43	Execution	No policy on e-government fund generation	0.2	0.5	0.1	Low
44	Execution	Failure to consider bringing in outside solutions	0.3	0.3	0.09	Low
45	Funding	Lack of funding for adequate security program	0.8	0.9	0.72	High
46	Funding	Lack of ability to predict Required resources and costs	0.8	0.8	0.64	High
47	Funding	Failure to consider the reallocation of staff savings	0.7	0.9	0.63	High
48	Funding	Insufficient savings to fund project beyond 2 years	0.7	0.7	0.49	Medium
49	Funding	Lack of funding causes incomplete implementation	0.7	0.7	0.49	Medium
50	Funding	Lack of funding forces agencies to choose between e-government and other projects	0.7	0.7	0.49	Medium
51	Funding	Failure to determine total cost of ownership	0.6	0.6	0.36	Medium
52	Funding	Failure to accurately quantify return on investment	0.5	0.7	0.35	Medium
53	Funding	Failure to conduct cost benefit analysis	0.5	0.7	0.35	Medium
54	Funding	Agencies unwilling to use savings to pay for infrastructure	0.5	0.5	0.25	Low

Ref #	Category	Risk Description	Probability	Consequence	P * C	Risk Levels
55	Funding	Failure to consider alternate funding mechanisms	0.3	0.5	0.15	Low
56	Legal	Contract renegotiation causes costs or schedule overrun	0.8	0.7	0.56	Medium
57	Legal	Lack of e-government legal expertise	0.7	0.4	0.28	Low
58	Legal	Potential for economic loss due to liability issues	0.7	0.4	0.28	Low
59	Legal	Increase in litigation concerning Internet	0.7	0.4	0.28	Low
60	Legal	Lawsuit stops or impedes progress	0.2	0.6	0.12	Low
61	Marketing	Lack of resources to develop and implement marketing plan	0.9	0.9	0.81	High
62	Marketing	Low usage due to inadequate marketing	0.9	0.5	0.45	Medium
63	Marketing	Lack of proper sponsorship and involvement	0.5	0.9	0.45	Medium
64	Marketing	Lack of effective marketing plan	0.5	0.8	0.4	Medium
65	Marketing	Failure to meet customer expectations because we haven't asked customers what they want	0.8	0.5	0.4	Medium
66	Marketing	Bad e-government PR	0.7	0.5	0.35	Medium
67	Marketing	Lack of continuity and buy in due to change in administration	0.3	0.9	0.27	Low
68	Marketing	Failure to embrace e-government causes retention of overhead	0.6	0.4	0.24	Low
69	Marketing	Failure to develop policy for advertisement	0.4	0.4	0.16	Low
70	Resources	State leadership has conflicting and competing priorities	0.9	0.9	0.81	High
71	Resources	Lack of staff expertise in security and privacy	0.8	0.9	0.72	High
72	Resources	Schedule slippage	0.9	0.6	0.54	Medium
73	Resources	Shortage of staff for development and implementation	0.9	0.5	0.45	Medium
74	Resources	Turnover of staff for development and implementation	0.7	0.5	0.35	Medium
75	Resources	Failure to maintain state's legacy environment during e-government implementation	0.3	0.8	0.24	Low
76	Resources	Insufficient 24-7 help desk support	0.7	0.3	0.21	Low

Ref #	Category	Risk Description	Probability	Consequence	P * C	Risk Levels
77	Security	External entities gain access to unauthorized data	0.9	0.9	0.81	High
78	Security	External entities gain access to unauthorized data and destroy	0.9	0.9	0.81	High
79	Security	Inadequate firewall protection	0.9	0.9	0.81	High
80	Security	Inadequate monitoring for security breaches	0.9	0.9	0.81	High
81	Security	Insufficient security procedures and policies	0.8	0.9	0.72	High
82	Security	Privacy violation	0.5	0.9	0.45	Medium
83	Security	Hackers are attracted due to increased visibility	0.8	0.4	0.32	Medium
84	Security	Customer perception of poor security	0.6	0.4	0.24	Low
85	Security	Unauthorized internal site access	0.2	0.7	0.14	Low
86	Technical	Lack of network and system capacity	0.8	0.8	0.64	High
87	Technical	Lack of network and system scalability	0.8	0.8	0.64	High
88	Technical	Inadequate help desk	0.8	0.8	0.64	High
89	Technical	Lack of robust search engine with business intelligence	0.8	0.8	0.64	High
90	Technical	Failure to implement effective and user friendly single sign on	0.7	0.9	0.63	High
91	Technical	Failure to manage bandwidth priorities between e-government and normal business requirements	0.7	0.9	0.63	High
92	Technical	Insufficient virus protection	0.7	0.7	0.49	Medium
93	Technical	Lack of network and system redundancy	0.4	0.8	0.32	Medium
94	Technical	Failure to integrate legacy systems with e-government	0.4	0.7	0.28	Low
95	Technical	Internet backbone failure	0.3	0.9	0.27	Low
96	Technical	Single sign on failure	0.3	0.9	0.27	Low
97	Technical	Failure to integrate existing network with e-government	0.3	0.7	0.21	Low
98	Technical	Failure to keep information current	0.3	0.5	0.15	Low
99	Technical	Low up time for site	0.1	0.9	0.09	Low
100	Technical	Site crashes	0.1	0.9	0.09	Low
101	Technology	Lack of access due to failure to address digital divide	0.9	0.9	0.81	High

Ref #	Category	Risk Description	Probability	Consequence	P * C	Risk Levels
102	Technology	Rapid change of technology causes integration failure	0.8	0.6	0.48	Medium
103	Technology	Backlash created by those without Internet access	0.8	0.5	0.4	Medium
104	Technology	E-government uses leading edge technology resulting in poor execution	0.8	0.4	0.32	Medium
105	Technology	Technology selections isolate potential users	0.7	0.4	0.28	Low
106	Technology	Can't keep pace with change in web industry	0.7	0.4	0.28	Low
107	Technology	Inaccurate expectations of technology solutions	0.4	0.4	0.16	Low
108	Training	Lack of training for employees	0.7	0.7	0.49	Medium
109	Training	Inadequate staff skill sets	0.7	0.5	0.35	Medium
110	Vendor	Inadequate vendor support	0.9	0.8	0.72	High
111	Vendor	Changing vendors during project lifespan	0.8	0.8	0.64	High
112	Vendor	Too many vendors in project	0.7	0.7	0.49	Medium
113	Vendor	New vendor products don't deliver expected functionality	0.6	0.6	0.36	Medium

3.0 Risk Analysis:

The team compiled a list of one hundred seven suggested preventive and contingency measures. These measures were then linked to high risks with exposure factors greater than .60. Comments were also added to identify risks that needed immediate or special attention and dependencies were also noted. This work is documented in figure 3.1 below:

Risk Management Worksheet

Figure 3.1

A description of high risks identified for the project, the probability of the risk occurring, the Impact of the risk on the project, and the suggested mitigation activities.

Ref #	Risk Category/ Event	Risk Exposure	Preventive Measures	Responsible Person	Comments
	Business Process				
1	Inadequate Organization Structure	0.81	1, 5, 18, 32, 33, 46, 57, 58, 59, 60, 62, 63, 64, 91, 92, 93, 94, 95		
2	Inability to I.D. individual customer and level of access	0.72	2, 4, 5, 12, 15, 32, 48, 66, 67, 68		This risk needs to be addressed early in the project and a decision made in the planning phase of the project. This risk will then be eliminated and should not create any further risk later in the project
	Communication				
12	Conflicts of ownership between agencies	0.81	1, 8, 11, 13, 14, 48, 54, 67, 73, 74, 81, 85, 86, 88, 90		This risk will have to be managed and revisited throughout the lifecycle of the project.
13	Lack of common language among customers, developers and implementers	0.72	5, 8, 11, 14, 37, 39, 44, 45, 55, 57, 58, 59, 65, 66, 67, 74, 75, 76, 77,81, 83, 85, 86, 88, 90, 100		This is a communication issue and should be addressed early and often
14	Lack of Cooperation between agencies	0.64	1, 8, 11, 13, 14, 48, 54, 67, 73, 74, 81, 85, 86, 88, 90		
	Execution				
24	Lack of sufficient architecture standards	0.81	5, 8, 19, 32, 48, 66, 67, 68, 73, 74, 75, 81, 86, 88, 105		This risk needs to be addressed early. Architecture standards must be identified prior to kickoff of this project

Ref #	Risk Category/ Event	Risk Exposure	Preventive Measures	Responsible Person	Comments
25	Lack of a plan for integration of services	0.64	1, 2, 16, 18, 20, 21, 34, 48, 52, 57, 60, 61, 64, 67, 68, 79, 80, 83, 90, 100		
26	Failure to establish a unique identifier for each citizen or agency	0.64	2, 5, 8, 13, 14, 32, 48, 65, 66, 67, 74, 78, 85, 86		This risk needs to be addressed early in the project and a decision made in the planning phase. This should eliminate the risk for the duration of the project.
	Funding				
45	Lack of funding to develop an adequate security program	0.72	17, 26, 27, 28, 30, 35, 39, 40, 41, 43, 55, 56		
46	Lack of ability to predict required resources and cost	0.64	21, 31, 32, 45, 48, 60, 61, 67, 79, 83, 91, 92		
47	Failure to consider the reallocation of staff savings	0.63	1, 33, 40, 41, 56		
	Marketing				
61	Lack of resources to develop and implement an effective marketing plan	0.81	26, 27, 28, 30, 51, 52, 53, 54, 56, 86, 90		
	Resources				
70	State leadership may have conflicting and competing priorities	0.81	9, 11, 15, 36, 41, 42, 43, 51, 54, 55, 56, 57, 86, 90		Early buy-in is required and continuous management of expectations will be required
71	Lack of staff expertise in security and privacy	0.72	32, 44, 45, 46, 48, 58, 59, 64, 66, 67, 68, 69, 70, 71, 72, 73, 75, 76, 88, 91, 94, 95, 105		Training should begin during the planning phase of the project in order to prepare staff for the kickoff of the project.

Ref #	Risk Category/ Event	Risk Exposure	Preventive Measures	Responsible Person	Comments
	Security				
77	External entities may gain access to unauthorized data	0.81	1, 5, 19, 32, 66, 67, 68, 69, 71, 73, 75, 78, 88,89		Security has been identified as a high priority item and needs to be addressed early and often throughout the lifecycle of this project
78	External entities may gain access to unauthorized data and destroy the data	0.81	1, 5, 19, 32, 66, 67, 68, 69, 70, 71, 73, 75, 78, 88, 89		
79	Inadequate firewall protection	0.81	5, 19, 32, 48, 52, 58, 59, 64, 66, 67, 68, 69, 71, 73		
80	Inadequate monitoring of security breaches	0.81	5, 19, 32, 48, 52, 58, 59, 64, 66, 67, 68, 69, 71, 73		
81	Insufficient security procedures and policies	0.72	1, 5, 19, 32, 66, 67, 68, 69, 70, 71, 73, 75, 78, 88, 89		This is dependent on implementation of architecture standards
	Technical				
86	Lack of network and system capacity	0.64	5, 12, 15 , 21, 32, 34, 60, 67, 68, 79, 80, 84		
87	Lack of network and system scalability	0.64	5, 12, 15 , 21, 32, 34, 60, 67, 68, 79, 80, 84		
88	Inadequate help desk	0.64	1, 58, 59, 64, 83, 90, 91, 92, 93		
89	Lack of robust search engine with business intelligence	0.64	5, 29, 32, 52, 59, 67, 68, 79, 84		
90	Failure to implement effective and user friendly single sign on	0.63	2, 7, 8, 13, 14, 32, 67, 85		This risk should be addressed early in the planning phase of the project and a decision made and adhered to. This should eliminate this risk for the duration of the project.
91	Failure to manage bandwidth priorities between e-gov and normal business	0.63	4, 18, 20, 21, 29. 34, 52, 60, 67, 79, 80		Plan and monitor throughout the lifecycle of the project.

Ref #	Risk Category/ Event	Risk Exposure	Preventive Measures	Responsible Person	Comments
	Technology				
101	Lack of access due to failure to address digital divide	0.81	4, 5, 7, 12, 32, 87, 89		
	Vendor				
110	Inadequate vendor support	0.72	10, 45, 46, 83, 96, 97, 98, 99, 100, 106		
111	Changing vendors during project lifespan	0.64	101, 104, 106, 107		

Suggested Preventive and Contingency Measures

1. Agencies implement business reengineering and reorganize to embrace new delivery system
2. Develop a strategy and process to create a unique customer identifier
3. Create a contingency plan to provide services if electronic delivery unavailable, i.e. disaster recovery, redundancy, security, etc.
4. Survey customers and hold focus groups to discover customer needs
5. Research other states experiences and best practices
6. Establish regular risk reviews and updates
7. Provide design for e-gov system flexibility to change with requirements
8. Establish OIT as the central point of e-gov
9. OIT communicates value of e-gov to agencies
10. Bring purchasing into the e-gov plan and process to assure ability to execute purchase contract
11. Develop inter-agency communication plan – show common gains and interests
12. Obtain feedback from customers on desires and expectations
13. Identify areas requiring inter-agency cooperation
14. Form inter-agency teams to address cooperation
15. Obtain feedback from legislators and agencies on expectations and desires
16. Build a bfg on progress to date and the plan for the future
    Present to internal and external
    Show benefits, convenience, savings, etc.
17. Show template for cost benefit analysis

18. Build a template of how a typical implementation might go
19. Expedite current architecture efforts (establish deadline)
    Communicate deadline and standards to all
20. Assign responsibility for creating an integration plan (involve all)
21. Each agency put together a schedule and plan of applications to be implemented
    Review by coordinating group
    Schedule regular status meetings to be tied in with risk management
22. Identify point of contact for each agency
    Have DMD establish editorial policies
23. Establish project baseline
24. Establish change management procedures (business community)
25. Establish risk reviews
26. Plan for and consider alternate funding – identify triggers
27. Consider advertising on web sites to supplement funding
28. Consider user fees to offset funding pitfalls
29. Consider 3rd party outsourcing for dissemination of data
30. Assign responsibility for search for grants to supplement Project GTS
31. Work with industry groups and vendors to estimate/predict costs (META, IBM, Gartner, etc.)
32. Look at existing models by other states – NASIRE, etc.
33. Develop a transition plan to offset duties of staff – use Data Center Consolidation as example
34. Plan for a phased implementation – identify portions that can slide if necessary.
35. Isolate program specifics that might qualify for some other sort of external funding
36. Promote technology and e-government to agencies and keep in the forefront – OIT/CIO
37. Promote value of project through internal marketing strategies
38. Rely on those groups to plan for TCO
39. Develop metrics and standards early on in the process regarding ROI
40. Conduct a cost benefit analysis plan and disseminate to appropriate people
41. Attempt to get agencies to commit up-front to reinvest project savings back into the project
42. Get buy-in to project and priority – internal marketing
43. Identify area and plan to AG
44. Find training opportunities
45. Identify contract support needed
46. Identify specific skills and expertise needed
47. Evaluate projects for legal risks
48. Research experience of other states and industry

49. Outsource professional for initial draft of marketing plan
50. Ensure implementation of plan
51. Ensure state officials are knowledgeable of e-gov marketing plan
52. Proper resources, proper implementation
53. Poll for input (as whole or representative group) to cover points important to them in e-gov (focus groups)
54. Right people marketing – effective marketing plan
55. Ensure knowledge of e-gov is understood, in importance, at high government level
56. Use marketing plan to shop how e-gov creates benefits
57. Ensure adequate knowledge for leadership to determine priorities for e-gov
58. Start developing training courses now to develop staff expertise
59. Utilize outside group(s) to provide initial expertise/knowledge transfer
60. Ensure appropriate/realistic schedules with consideration of resources
61. Look to other organizations who have implemented this type of project for assistance in scheduling
62. Review salary requirements to enhance state vs. private industry (more competitive)
63. Increase recruiting activities
64. Provide adequate staffing/training
65. Establishment of e-gov operational procedures (software, funding)
66. Develop architecture and infrastructure plans with security in mind from the beginning
67. Use other models, success and failures and incorporate lessons learned into our strategy (KBI example)
68. Gain input from vendors such as META, IBM, etc.
69. Incorporate tests with federal and private companies into the plan to hack and fix problem areas (Search Group, FBI, private)
70. Have a plan for data recovery in the event that it happens
71. Include monitors and QA in the process plan for identification of when a breach occurs
72. Develop a communication plan for disseminating cause and results if attack to those impacted and those responsible for security
73. Identify the entity responsible for security (security group) up front
74. Publish policies and procedures prior to implementation
75. Develop a user policy or privacy violation – consult legal staff
76. Include security measures in marketing strategy
77. Internal marketing and awareness (communicated)
78. Develop policies and procedures and actions which specifically deal with this
79. Implement a study involving all stakeholders (MOREnet, OA, etc.) for capacity and scalability
80. Develop a plan that follows study recommendations

81. Ensure architecture compatibility up-front
82. Coordinate group to review plan
83. Assign responsibility of help desk to work with vendors to establish help desk, training of staff early in project (users, developers involved)
84. Search engine – build vs. buy decision early
85. Assign responsibility for single sign-on to involve all stakeholders to get buy-in
86. Communicate with all agencies via ITAB members
87. Provide for alternative methods of access (i.e., kiosk, AVR, etc.)
88. Create, implement and adhere to IT architecture and standards
89. Provide necessary training to IT community to stay current with change in the Web industry
90. Use communication strategies to manage expectations
91. Research skills required in other states
92. Inventory skills in MO
93. Get MOTEC involved
94. Build training plan
95. Build or contract specific courses
96. Inadequate vendor support
97. Changing vendors during project life span
98. Too many vendors in project
99. New vendor projects don't deliver expected functionality
100. Manage vendor activities
101. Get procurement into project early on
102. Do an RFI
103. Establish team to write RFP from multi-agencies
104. Research other states contracts
105. Put Standards/Architecture in RFP
106. Decision on one vs. many vendors
107. Award secondary and possibly tertiary contracts.

4.0 Conclusion and Summary

This is the initial risk assessment for this project and the overall risk exposure indicates it to be a medium risk project. Risk management is an iterative process and these risks will be continually monitored at regularly scheduled meeting throughout the lifecycle of this project. A meeting is being scheduled in early April to update this plan. Many risks in the Security and Technical categories that were identified as high-risk items will be addressed at this time. The mitigation strategies for these risks are being addressed at this time and are critical to the success of this project.